

## GRC Automation Platform Policy Definition and Enforcement



### AccuKnox Governance, Risk, and Compliance Platform:

- Define Policy Rules
- Enforce Compliance
- Proactive and Automated Remediation
- Real-time Monitoring and Auditing
- Comprehensive Reporting
- Predefined rules for CIS1, CIS2, HIPAA, PCI-DSS, MITRE, NIST

### 1 GOVERNANCE

- Multi-Tenancy, RBAC controls, Separation of Duties
- Dashboard for definitions and runtime monitoring
- Continuous Logging, Monitoring, Alert & Audit
- Integrates into existing SOCs

### Comprehensive Coverage:

To support coverage for *Digital Transformation Journey*, we have controls and technical “know-how” to secure the following

- Modern Infrastructure – Pubic, Private, Hybrid Clouds
- Modern Workload – Kubernetes, Containers
- Traditional Workload – VM/Bare Metal, Docker
- Datacenter / On-Premise Support

### Multi Tenancy, RBAC, Organizational Isolation:

- Isolated and Secured at organization level from others
- Segment different domains based on Tenants in the organization
- Temporal Invite access to users and revoke when not needed
- Define RBAC in the Tenants for different teams working on a same project such as Monitoring Team, R&D Team, Management Team etc.
- Application Behavior & Real time Monitoring & Multi-Cloud View

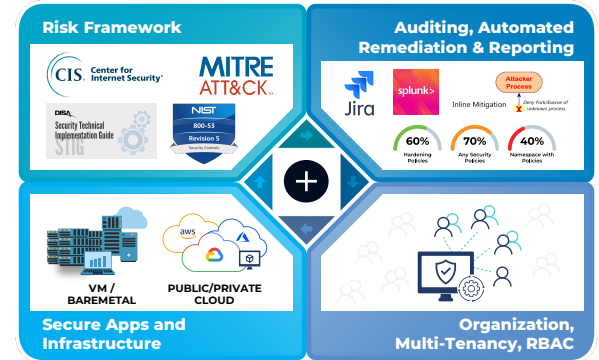
### 2 RISK

- Auto-detect Security Posture for specific applications
- Automated generation of baseline and policy control
- Risk / compliance based prioritization of the issues
- Workflow automation, monitoring, alerting, blocking on violation,
- Automated audit logs

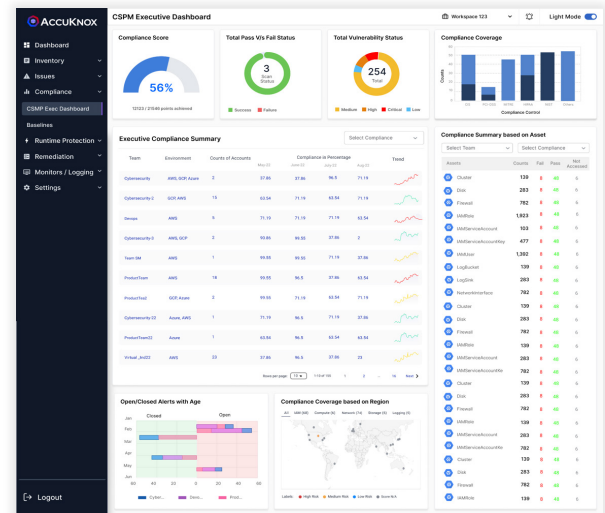
- Auto-Discovers – Compliance Posture
- Continuous Security & Assessment with Audit or Auto Remediate
- Violations such as File Integrity Monitoring & System and Information Integrity
- Deep Telemetry and Forensics on Logs, events and alerts

### Risk-based Prioritization:

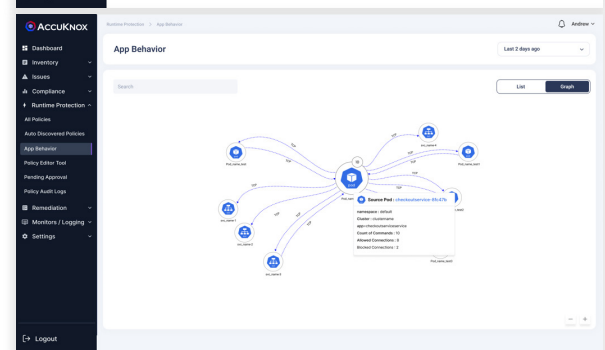
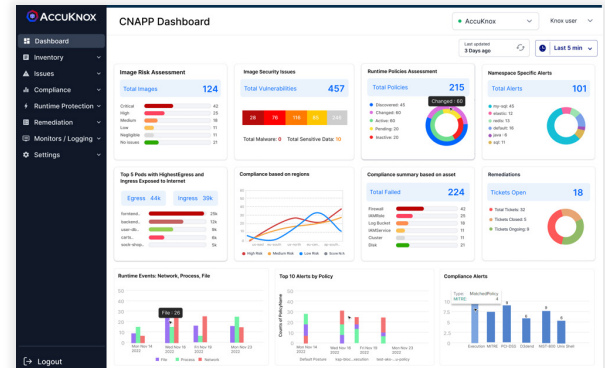
- Prioritize Vulnerabilities Risk based on factors such as – Network Exposed? Exploitable? Used at Runtime?
- Ingest vulnerabilities from multiple data sources and prioritize among them to handle critical vulnerability
- System behavior is based on adherence to policy rules
- Automatically block non-confirming actions
- Automatically alerts non conformance
- Audit every events and generate Logs



### Cloud, Kubernetes Posture Management (CPSM, KPSM)



### Cloud Workload Protection Platform (CWPP)



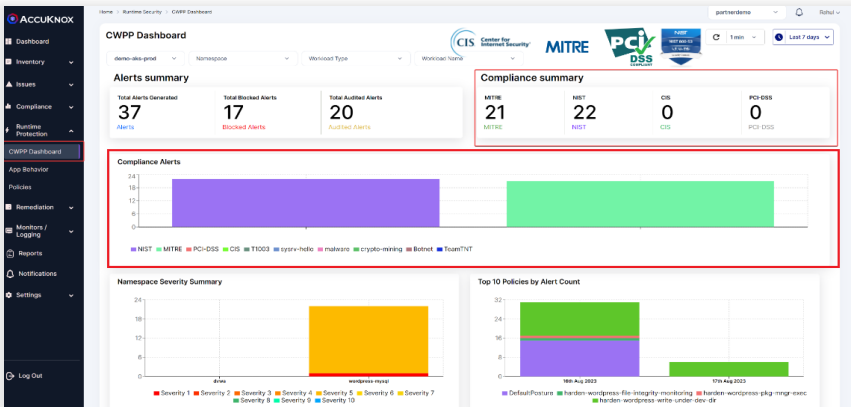
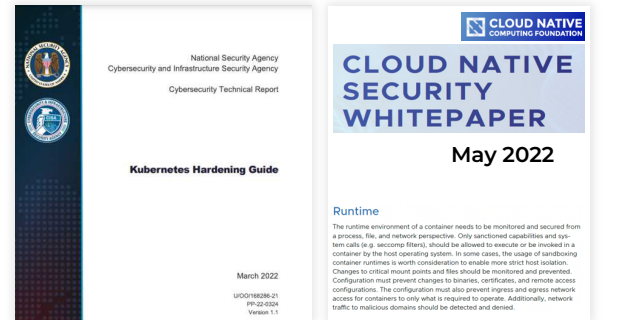
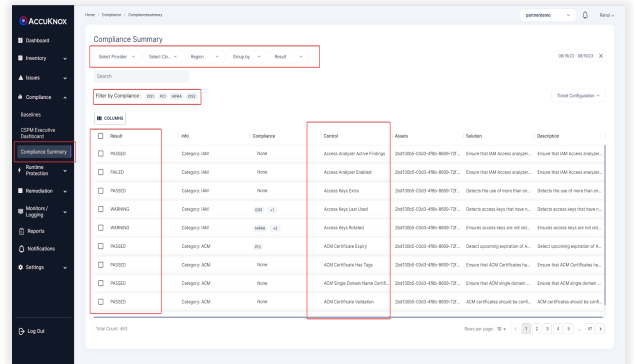
## 3 COMPLIANCE

- System and application compliance with CIS1, CIS2, HIPAA, PCI-DSS, MITRE, NIST
- On demand Compliance Report
- Continuous, Periodic and On-demand scan
- Audit / Block based Remediation for violation
- Forensics, Audit Trail and RCA

GRC ROADMAP

<b>Onboarding</b>	Cloud Infra Inventory	Onboard App workloads	CI Pipeline Integration
<b>Auto-Discover Posture</b>	GH repo security status	App security posture & vulnerability	Issues in Cloud Infra
<b>Baseline</b>	Cloud -> current Cloud Posture	GH repo -> scan	APP -> auto generated policies
<b>Continuous Observability</b>	Multi-Cloud View	Application Behavior	Integration to SIEM tools
<b>Mode of Enforcement</b>	Auto Remediate and report violations	Detect Drift in cloud and get alerts	Audit and report suspicious behavior
<b>Reporting, Analytics &amp; Auditing</b>	Reporting for 3PAO	Real-time Log Monitoring	Audit Trail & Deep Telemetry

## Rigorous Cloud Security Standards Compliance



“Zero Trust run-time Cloud Security has become an organizational imperative for Companies and Governments. AccuKnox’ highly differentiated approach, their eBPF foundations and their seminal innovations developed in partnership with Stanford Research Institute [SRI] positions them very well to deliver a highly differentiated and efficient Zero Trust Cloud Security platform”

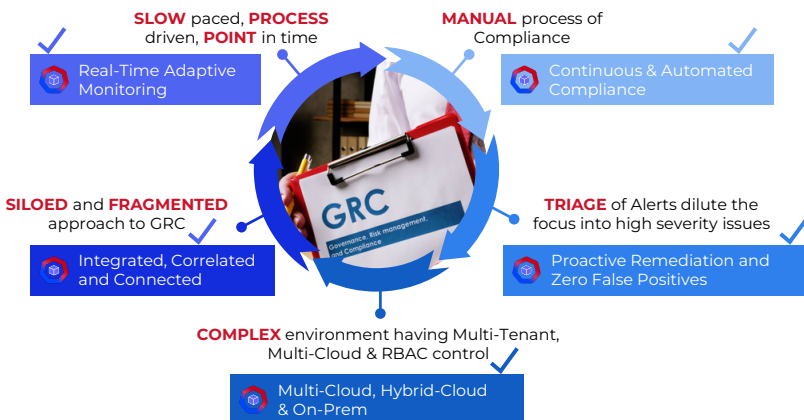
**Frank Dickson, Vice President Security and Trust, IDC**

## Customer Accolades

“AccuKnox has one of the most comprehensive, modern, Cloud Native CNAPP offering”  
**— Top 25 SAAS Software Company**

“AccuKnox and its capabilities in the areas of run-time security enforcement is unique. We like the fact that it is a CNCF Supported project. It has the support of the global community.” **— Top 10 Telco**

“While researching solutions to the increasing and advanced attacks in the Cloud, we were impressed with AccuKnox’ approach to Zero Trust and NSA/CISA hardening guidelines. With their contributions OpenSource, AccuKnox is a clear winner.”  
**— Top 50 Cloud Native Unicorn**



## About AccuKnox

AccuKnox provides a Zero Trust Cloud Native Application Security (CNAPP) platform. AccuKnox is built in partnership with SRI (Stanford Research Institute) and is anchored on seminal inventions in the areas of: Container Security, Anomaly Detection and Data Provenance. AccuKnox can be deployed in Public and Private Cloud environments.

[www.accuknox.com](http://www.accuknox.com) [contact@accuknox.com](mailto:contact@accuknox.com)